UCZELNIA BIZNESU
I NAUK STOSOWANYCH
VARSOVIA

UCHWAŁA SENATU nr 19/07/2026
Uczelni Biznesu i Nauk Stosowanych „Varsovia"
z dnia 10 lipca 2026 roku

w sprawie przyjęcia znowelizowanego programu studiów podyplomowych „Cyberbezpieczeństwo"

Na podstawie § 23 pkt 7 w związku z § 26 ust. 1 statutu Uczelni Biznesu i Nauk Stosowanych „Varsovia", uchwala się, co następuje:

§ 1.

Senat Uczelni Biznesu i Nauk Stosowanych „Varsovia" ustala znowelizowany program studiów podyplomowych „Cyberbezpieczeństwo", stanowiący załącznik nr 1 do niniejszej uchwały.

§ 2.

Program, o którym mowa w § 1, stosuje się do edycji studiów podyplomowych rozpoczynających się po dniu wejścia w życie niniejszej uchwały.

§ 3.

Uchwała wchodzi w życie z dniem podjęcia.

REKTOR
adw. Magdalena Stryja

Przewodnicząca Senatu Uczelni Biznesu i Nauk Stosowanych „Varsovia"
Rektor adw. Magdalena Stryja

Opracowali: dr Monika Wild – Urbanek, dr Paweł Łabuz

Uczelnia Biznesu i Nauk Stosowanych „Varsovia”

Warszawa, 10.07.2026

PROGRAM

STUDIÓW PODYPLOMOWYCH

CYBERBEZPIECZEŃSTWO (210 h | 30 ECTS | 2 semestry)

zgodnie z wytycznymi zawartymi w:

- Ustawie z dnia 20 lipca 2018 r. – *Prawo o szkolnictwie wyższym i nauce* (tekst jednolity, Dz.U. 2024 r. poz. 1571).
- Rozporządzenia Ministra Nauki z dnia 18 lipca 2024r. *zmieniające rozporządzenie w sprawie dokumentów wydawanych w związku z przebiegiem lub ukończeniem studiów podyplomowych i kształcenia specjalistycznego* (Dz.U. 2024 poz. 1103).
- Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, tekst ujednolicony Kancelarii Sejmu, stan na 24.03.2026; uwzględniono m.in. organizację KSC, role CSIRT, obowiązki podmiotów i zarządzanie incydentami.
- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. (NIS2), Dz.Urz. UE L 333 z 27.12.2022. https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng
- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. (NIS2), Dz.Urz. UE L 333 z 27.12.2022. https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng
- ENISA, ENISA Threat Landscape 2025; raport obejmuje 4875 incydentów z okresu 01.07.2024-30.06.2025.

https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

- NIST, The NIST Cybersecurity Framework (CSF) 2.0, 26.02.2024. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
- ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection - Information security management systems - Requirements. https://www.iso.org/standard/27001
- ENISA, European Cybersecurity Skills Framework Role Profiles, 19.09.2022; oraz ENISA, Mapping NIS2 obligations to ECSF role profiles, czerwiec 2025. https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles

Informacje ogólne

Nazwa studiów podyplomowych	**SUICYDOLOGIA**
Nazwa jednostki prowadzącej studia	**Uczelnia Biznesu i Nauk Stosowanych „Varsovia"**
Termin rozpoczęcia	**sem. zimowy roku akad. 2026/2027**
Liczba semestrów	2
Ogólna liczba punktów ECTS	30
Ogólna liczba godzin zajęć dydaktycznych	210
Ogólna liczba godzin zajęć warsztatowych i praktycznych	120 godz.
Przypisanie poziomu Polskiej Ramy Kwalifikacji	PRK 7 charakterystyk drugiego stopnia
Wymagane kwalifikacje poprzedzające	Kwalifikacja pełna co najmniej na poziomie 6 PRK uzyskana w systemie szkolnictwa wyższego i nauki. Rekomendowane są studia lub doświadczenie w obszarze: informatyka, bezpieczeństwo, administracja, prawo, zarządzanie, ochrona informacji, zarządzanie kryzysowe, sektor publiczny, służby, infrastruktura krytyczna, compliance albo IT.

Cel studiów	Celem studiów podyplomowych „Cyberbezpieczeństwo" jest przygotowanie słuchaczy do rozumienia, planowania, wdrażania, monitorowania i audytowania podstawowych oraz średnio zaawansowanych działań z zakresu cyberbezpieczeństwa w organizacjach publicznych i prywatnych. Program łączy perspektywę prawną, organizacyjną, menedżerską, techniczną i śledczą. Zakres programu obejmuje w szczególności: krajowy system cyberbezpieczeństwa, wymagania NIS2, zarządzanie ryzykiem, zarządzanie incydentami, współpracę z CSIRT, ochronę informacji i danych, bezpieczeństwo sieci i systemów, bezpieczeństwo chmury, OSINT i cyber threat intelligence, informatykę śledczą, audyt, bezpieczeństwo infrastruktury krytycznej oraz aktualne zagrożenia związane ze sztuczną inteligencją, deepfake, socjotechniką i operacjami wpływu.
Profil absolwenta/absolwentki studiów podyplomowych	Absolwent studiów posiada uporządkowaną, interdyscyplinarną wiedzę oraz praktyczne kompetencje potrzebne do wspierania organizacji w obszarze cyberbezpieczeństwa. Program nie tworzy odrębnych uprawnień zawodowych poza świadectwem ukończenia studiów podyplomowych; przygotowuje do wykonywania zadań organizacyjnych, analitycznych, compliance, koordynacyjnych i podstawowych zadań technicznych w granicach posiadanych kwalifikacji zawodowych. • rozumie podstawowe i współczesne pojęcia cyberbezpieczeństwa, cyberodporności, zarządzania ryzykiem i bezpieczeństwa informacji; • zna podstawowe obowiązki organizacji wynikające z KSC, NIS2 oraz zasad ochrony informacji, w tym ochrony danych osobowych i tajemnic prawnie chronionych; • potrafi identyfikować aktywa, zagrożenia, podatności i ryzyka oraz dobierać adekwatne środki organizacyjne i techniczne; • potrafi uczestniczyć w obsłudze incydentu, przygotować podstawowy raport incydentu i współpracować z właściwymi osobami lub zespołami, w tym CSIRT; • potrafi zabezpieczać i dokumentować podstawowe ślady cyfrowe z zachowaniem zasad legalności, integralności i rozliczalności; • potrafi wykorzystywać OSINT, CTI i MITRE ATT&CK do podstawowej analizy zagrożeń i zachowań adwersarzy; • zna znaczenie audytu, zgodności, ciągłości działania, kopii zapasowych, zarządzania podatnościami, bezpieczeństwa łańcucha dostaw i szkoleń użytkowników;

	• rozumie nowe ryzyka związane z AI, deepfake, prompt injection, LLM Security, automatyzacją ataków, dezinformacją, infrastrukturą krytyczną i systemami OT/ICS/SCADA; Jest gotów do pracy interdyscyplinarnej z działem IT, kierownictwem organizacji, prawnikami, inspektorem ochrony danych, audytorami, administracją publiczną, służbami i podmiotami zewnętrznymi

Warunek ukończenia studiów i otrzymania świadectwa	Osiągnięcie wszystkich efektów uczenia się i zaliczenie wszystkich przedmiotów, zawartych w planie studiów, a także wykonanie pracy końcowej, zgodnie z kryteriami oceny, podanymi w karcie przedmiotu
Dokument potwierdzający nabyte kwalifikacje	Świadectwo ukończenia studiów podyplomowych z zakresu prowadzenia Terapii Zaburzeń Więzi w: **języku polskim** • **świadectwo ukończenia studiów podyplomowych**(zgodnie art. 164 ustawy z dnia 20 lipca 2018r. – Prawo o szkolnictwie wyższym i nauce (Dz. U. poz. 1668 oraz Rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z dnia 12 września 2018 r. w sprawie dokumentów wydawanych w związku z przebiegiem lub ukończeniem studiów podyplomowych i kształcenia specjalistycznego – 19 września 2018 r. Poz. 1791) **lub/i języku angielskim** (fakultatywnie na życzenie)

	• **świadectwo ukończenia studiów podyplomowych** (zgodnie art. 164 ustawy z dnia 20 lipca 2018r.- Prawo o szkolnictwie wyższym i nauce (Dz. U. poz. 1668 oraz Rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z dnia 12 września 2018 r. w sprawie dokumentów wydawanych w związku z przebiegiem lub ukończeniem studiów podyplomowych i kształcenia specjalistycznego- 19 września 2018 r. Poz. 1791)

Objaśnienia oznaczeń:

- SP7_CB - efekty uczenia się dla studiów podyplomowych „Cyberbezpieczeństwo" na poziomie PRK 7;
- W - wiedza; U - umiejętności; K - kompetencje społeczne;
- P7S_WG, P7S_WK, P7S_UW, P7S_UK, P7S_UO, P7S_UU, P7S_KK, P7S_KO, P7S_KR - symbole charakterystyk drugiego stopnia Polskiej Ramy Kwalifikacji dla poziomu 7.

Efekty uczenia się

Symbol	Po ukończeniu studiów absolwent zna i rozumie / potrafi / jest gotów do	Odniesienie do PRK 7
SP7_CB_W01	zna i rozumie terminologię cyberbezpieczeństwa, cyberodporności, bezpieczeństwa informacji, incydentu, podatności, zagrożenia i ryzyka cybernetycznego	P7S_WG
SP7_CB_W02	zna i rozumie podstawowe regulacje prawne dotyczące cyberbezpieczeństwa, w tym KSC, NIS2, ochronę danych osobowych, ochronę tajemnic prawnie chronionych oraz podstawy odpowiedzialności za cyberprzestępczość	P7S_WK
SP7_CB_W03	zna zasady zarządzania ryzykiem, zgodnością, ciągłością działania, bezpieczeństwem łańcucha dostaw oraz cyberbezpieczeństwem w organizacji	P7S_WG, P7S_WK
SP7_CB_W04	zna podstawowe standardy i ramy odniesienia wykorzystywane w cyberbezpieczeństwie, w szczególności ISO/IEC 27001:2022, NIST CSF 2.0, ECSF oraz MITRE ATT&CK	P7S_WG
SP7_CB_W05	zna podstawowe środki techniczne zabezpieczania sieci, systemów, usług chmurowych,	P7S_WG

Symbol	Po ukończeniu studiów absolwent zna i rozumie / potrafi / jest gotów do	Odniesienie do PRK 7
	tożsamości cyfrowej, kryptografii, kopii zapasowych i zarządzania podatnościami	
SP7_CB_W06	zna zasady obsługi incydentu, raportowania, współpracy z CSIRT, dokumentowania działań i przygotowania organizacji do reagowania oraz odtwarzania po incydencie	P7S_WG, P7S_WK
SP7_CB_W07	zna podstawy informatyki śledczej, zabezpieczania dowodów cyfrowych, zachowania integralności materiału oraz granice wykorzystania materiału cyfrowego	P7S_WG, P7S_WK
SP7_CB_W08	zna aktualne kategorie zagrożeń: ransomware, DDoS, phishing, socjotechnikę, deepfake, ataki na chmurę, zagrożenia dla OT/ICS/SCADA, operacje wpływu oraz ryzyka związane ze sztuczną inteligencją	P7S_WG, P7S_WK
SP7_CB_U01	potrafi identyfikować aktywa, podatności, zagrożenia i ryzyka oraz proponować adekwatne środki organizacyjne, prawne i techniczne	P7S_UW
SP7_CB_U02	potrafi opracować podstawowy rejestr ryzyk, procedurę bezpieczeństwa informacji, procedurę obsługi incydentu albo plan działań naprawczych	P7S_UW, P7S_UO
SP7_CB_U03	potrafi przeprowadzić podstawową analizę incydentu, przygotować raport z incydentu oraz zaplanować działania minimalizujące skutki zdarzenia	P7S_UW, P7S_UK
SP7_CB_U04	potrafi zabezpieczyć i opisać podstawowy materiał cyfrowy z zachowaniem zasad integralności, poufności, legalności i rozliczalności	P7S_UW
SP7_CB_U05	potrafi wykorzystać OSINT, CTI oraz mapowanie MITRE ATT&CK do rozpoznawania i opisywania zachowań adwersarzy	P7S_UW
SP7_CB_U06	potrafi zaprojektować podstawowe działania świadomościowe, antyphishingowe i szkoleniowe dla użytkowników oraz kadry zarządzającej	P7S_UK, P7S_UO
SP7_CB_U07	potrafi ocenić podstawowe zabezpieczenia sieci, chmury, tożsamości cyfrowej i procesów organizacyjnych oraz wskazać priorytety poprawy bezpieczeństwa	P7S_UW
SP7_CB_U08	potrafi przygotować projekt końcowy obejmujący plan zarządzania cyberbezpieczeństwem, audyt, analizę ryzyka albo scenariusz reakcji na incydent	P7S_UW, P7S_UO, P7S_UU
SP7_CB_K01	jest gotów do działania zgodnie z prawem, etyką, zasadą minimalizacji danych i poszanowaniem praw osób, których dane lub systemy są analizowane	P7S_KR
SP7_CB_K02	jest gotów do rozpoznawania granic własnych kompetencji oraz kierowania spraw do specjalistów, administratorów systemów, CSIRT, organów ścigania lub audytorów	P7S_KK, P7S_KR
SP7_CB_K03	jest gotów do pracy interdyscyplinarnej oraz komunikowania ryzyk w sposób zrozumiały dla kadry technicznej, prawnej, zarządczej i administracyjnej	P7S_KO, P7S_KR

Symbol	Po ukończeniu studiów absolwent zna i rozumie / potrafi / jest gotów do	Odniesienie do PRK 7
SP7_CB_K04	jest gotów do stałego aktualizowania wiedzy w związku z szybkim rozwojem technologii, zmianą zagrożeń i zmianami regulacyjnymi	P7S_KK
SP7_CB_K05	jest gotów do odpowiedzialnego postępowania z informacjami wrażliwymi, dowodami cyfrowymi, tajemnicami prawnie chronionymi oraz wynikami testów bezpieczeństwa	P7S_KR

PLAN STUDIÓW

Łączna liczba godzin zajęć wynosi 210, w tym 90 godzin wykładów oraz 120 godzin ćwiczeń, warsztatów lub laboratoriów problemowych. Łączna liczba punktów ECTS wynosi 30. **Plan ma charakter praktyczny: ponad połowa godzin kontaktowych ma formę ćwiczeniową, warsztatową lub projektową.**

(W – wykład, Ć – ćwiczenia).

Lp.	Przedmiot	Sem.	W	Ć	Razem	ECTS
1	**Podstawy cyberbezpieczeństwa i ekosystem zagrożeń**	1	5	5	10	1
2	**Postępowanie z incydentem informatycznym**	1	7	8	15	3
3	**Prawne aspekty cyberbezpieczeństwa, ochrony informacji i danych osobowych**	1	6	4	10	1
4	**Zarządzanie cyberbezpieczeństwem, ryzykiem i zgodnością organizacji**	1	6	9	15	3
5	**Zabezpieczanie dowodów cyfrowych na potrzeby analiz śledczych**	1	5	5	10	2
6	**Bezpieczeństwo sieci, systemów i usług internetowych**	1	5	10	15	2
7	**Technologie zabezpieczania, kryptografia i zarządzanie tożsamością**	1	4	6	10	1
8	**Bezpieczeństwo chmury i usług cyfrowych**	1	4	6	10	1
9	**OSINT, rozpoznanie i cyber threat intelligence**	1	4	6	10	1
10	**Socjotechnika, cybermanipulacja i operacje wpływu**	2	5	5	10	1
11	**Postępowanie z incydentem informatycznym i współpraca z CSIRT**	2	5	10	15	2
12	**Zarządzanie incydentem i kryzysem cybernetycznym**	2	5	10	15	2
13	**Informatyka śledcza i zabezpieczanie dowodów cyfrowych**	2	5	10	15	2
14	**Monitorowanie, wykrywanie i analiza ataków**	2	4	6	10	2
15	**Cyberprzestępczość i odpowiedzialność prawna**	2	6	4	10	1
16	**Bezpieczeństwo infrastruktury krytycznej i odporność usług**	2	4	6	10	1
17	**Sztuczna inteligencja w cyberbezpieczeństwie: AI Security, LLM Security, deepfake i prompt injection**	2	5	5	10	1
18	**Audyt i zgodność w cyberbezpieczeństwie**	2	5	5	10	3
		SUMA	**90**	**120**	**210**	30

Sposób weryfikacji efektów uczenia się

- testy wiedzy lub krótkie sprawdziany problemowe z przedmiotów teoretycznych;
- analiza przypadku dotyczącego incydentu, naruszenia bezpieczeństwa lub ryzyka organizacyjnego;
- ćwiczenia z klasyfikacji incydentu, przygotowania zgłoszenia, komunikacji i raportu końcowego;
- zadanie praktyczne z OSINT/CTI wykonane wyłącznie na legalnych, otwartych i dydaktycznych materiałach;
- analiza logów, przykładowych alertów lub artefaktów cyfrowych w środowisku dydaktycznym;
- symulacja tabletop exercise dotycząca incydentu lub kryzysu cybernetycznego;
- projekt polityki, procedury, rejestru ryzyk, planu audytu albo planu ciągłości działania;
- projekt końcowy i jego omówienie.